REMARKS/ARGUMENTS

This paper is filed in response to the Examiner's Report of January 26, 2007, a response to which is due to be filed by April 26, 2007. Accordingly, the Applicant believes no fees are due as a result of this submission, in particular extension of time fees. In event the Applicant is mistaken, the Commissioner is hereby authorized to deduct any fees required and, in particular, extension of time fees, from our Deposit Account No. 13-2400, in this and future replies.

No amendments have been made by way of this submission. Claims 1-34 remain pending.

In the Examiner's Report of January 26, 2007, claims 1-34 were rejected based on various cited references. In particular, claims 1-6, 9-18, 21-28, and 31-34 were rejected under U.S.C. § 102(e) as being anticipated by US patent Publication No. 2003/0005118 (Williams et al.). The remaining claims were rejected as being obvious under 35 U.S.C. § 103(a) having regard to Williams in combination with US Patent No. 5,907,621 (Bachman et al.). The Applicant has carefully considered the Examiner's rejections, but respectfully traverses the art-based rejections for the reasons that follow.

The present application is directed to a system and method for secure session management in a web farm. The web farm includes at least two servers containing web pages that may be accessed by remote client devices. A concern with session management in the context of web farms is that the servers within a web farm may operate on different platforms, which may lead to different encoding techniques with regard to session tokens as between different servers. Accordingly, a problem may result if a session is initiated between a client and a first server and a session token is generated and encrypted by the first server and transmitted to the client device. A subsequent request by the client device for a web page that is located on a second server may be re-directed by the first server to the second server. Unfortunately,

the second server may be unable to decrypt the encrypted session token that accompanies the redirected request.

To address this issue, the present application proposes a common session database and a session management web service accessible to each of the servers in the web farm. The present application also proposes a method whereby the first server, upon receiving the request for a web page located on a second server, decrypts the session token and redirects the request to the second server along with the decrypted session token. In this manner, the second server does not encounter the problem of an encrypted session token which it cannot decrypt. The second server may then authenticate the session token via the session management web service and respond to the client request accordingly. To maintain security, in some embodiments, the second server creates a new session token, encrypts the new session token and transmits the new session token to the client device along with the requested web page.

The Williams et al. reference, by contrast, does not relate to web farms. Williams et al. describe a protected domain (200) which includes a protected server (206) that contains content that may be requested by a client device (204). The domain (200) may also contain a cookie distribution centre (CDC)(2002). Reference may be made to Figures 2A-2D. Williams et al. addresses the issue of session management using session tokens. Williams et al. distinguish between a domain token and a service token. A domain token represents a client's identity and entitlement to access a secure domain (200). The domain token may be valid for as long as the client accesses the domain. A service token represents a client's entitlement to a specific service. A domain token may be used with any service within a domain that recognizes domain token, but a service token is specific to a particular service. Reference may be made to paragraph [0049]. Domain tokens are generated and authenticated by the CDC (202). Service tokens are generated and authenticated by the protected server (206).

The Williams et al. reference describes a session management process in which the client (204) sends a login request (210) to CDC (202). At this stage, the client (204) has no tokens. The CDC (202) engages in a login process with the client (204) which will result in generation of a single-use domain token (216) which is returned to the client. At a later stage, the client (204) may send a request (220) for a protected service/resource to the protected server (206). The request (220) includes the single-use domain token (216) that was received from the CDC (202). In response to this request, the protected server (206) sends the client's single-use domain token (216) and the protected server's own domain token to the CDC (202) for authentication. The CDC authenticates/validates the client's single-use domain token and the protected servers single-use domain token, generates client credentials and refreshes the client's single-use domain token and the protected server's single-use domain token. The refreshed tokens are returned to the protected server (206), which then sends the refreshed client single-use domain token back to the client along with the requested service/resource. With that response, the protected server (206) also generates and sends a single-use service token.

Subsequent requests from the client will include the refreshed single-use domain token and the single-use service token. The protected server validates the single-use service token, and refreshes the single-use service token. In some embodiments, it may also send the refreshed domain token to the CDC (202) in order to obtain another refreshed domain token. The protected server (206) then responds to the client request along with the refreshed single-use service token and, in some embodiments, the another refreshed domain token.

It will be appreciated that the Williams et al. reference does not describe a web farm environment in which requests for resources located on the second server may be received by a first server with an encrypted session token that the first server must decrypt and pass to the second server along with the redirected request. The Examiner points to paragraph [0067] as an example of a redirect. Paragraph [0067] relates to the case wherein a client has no tokens and requests access to a

protected resource. In a situation, the protected server (206) redirects the client to the CDC (202) to perform the login process described above so as to obtain a single-use domain token. This does not equate to a client request for a web page located on the CDC nor does it involve an encrypted token, a step of decrypting the encrypted token, or, indeed, any tokens. This paragraph specifically addresses the situation in which the client has no tokens.

Claim 1 of the present application specifies a method of secure session management for a web farm, in which the web farm includes a first server and a second server, and the second server has a requested web page. The method includes steps of receiving, at the first server, a request for the requested web page from a browser, the request including an encrypted session token. The Examiner points to paragraphs [0016], [0019], [0050], and [0051]. However, these paragraphs or any other portions of the Williams et al. reference do not describe the receipt of a request at a first server for a requested web page located on a second server wherein the request includes an encrypted session token. To the extent that the client (204) sends a request for a web page, it sends that request to the protected server (206) for web pages located on the protected server (206). Williams et al. do not describe a second server containing resources that may be requested by the client. The CDC (202) described by Williams is not a second server having a requested web page, as described and claimed in the present application. The CDC performs a login process in order to authentic the client and performs domain token generation and management. In this regard, it may be better equated with the session management web service described in the present application, although there are significant distinctions between the two.

The method claimed in claim 1 also includes a step of decrypting the session token at the first server to obtain a session token, and redirecting the request to the second server, along with the session token. The Examiner points to paragraphs [0067] and [0020] of the Williams et al. reference. As noted-above, paragraph [0067] relates to redirecting requests for access to a resource on the protected

server (206) from the protected server to the CDC (206) in a situation in which the client (204) has no tokens. Accordingly, in Williams et al. there can be no step of redirecting a request to the second server along with the session token, as claimed in claim 1 of the present application.

For at least the foregoing reasons, the Applicant respectfully submits that the Williams et al. reference fails to teach or suggest a number of significant limitations contained in claim 1 of the present application. Accordingly, the Applicant respectfully suggests that claim 1 and all claims dependent thereupon is both novel and non-obvious over the Williams et al. reference, taken alone or in combination with the Bachman et al. reference.

Claim 13 of the present application is a claim to a system for secure session management including a first server having a first request handler for receiving a request and encrypting an encrypted session token to produce a session token, and a second server including a requested web page. As best the Applicant can tell, the Examiner purports to find multiple servers in paragraph [0013] of the Williams et al. reference wherein it states that, "[s]ince cookies are supported by all commercial Web browsers and servers, cookies are frequently used for detailed session management, such as tracking user movement within Websites." This sentence appears in the background of the invention section of the Williams et al. reference to suggest that use of cookies for secure session management has certain vulnerabilities. Nowhere within the disclosure of the Williams et al. reference does it actually describe a first server and a second server wherein the first server includes a first request handler for receiving a request and encrypting an encrypted session token and a second server that includes a requested web page. Moreover, claim 13 of the present application specifies that the first request handler is configured to redirect the request to the second server and transmit the session token to the second server. To the extent that the Examiner relies upon paragraph [0067] as teaching this feature, the Applicant repeats the comments set out above in connection with paragraph [0067]. The Williams et al. reference fails to teach a

second server having a requested web page and any component or device for redirecting the request from a first server to a second server along with a decrypted session token. Paragraph [0067] relates solely to redirecting a client request for a resource to the CDC (202) to initiate a login process when the client has no token.

For all the foregoing reasons, the Applicant respectfully submits that the Williams et al. reference fails to teach one or more claim limitations found in claim 13 of the present application. Therefore, claim 13 of the present application is novel and non-obvious over the Williams et al. reference, taken alone or in combination with Bachman et al. The Applicant also submits that the claims depending upon claim 13 are patentably distinguishable over Williams et al. for the same reasons.

With regard to claim 23 and all claims dependent thereupon, the Applicant repeats or relies upon its submissions in connection with claim 1 and all claims dependent thereupon.

In short, the Applicant respectfully submits that the Williams et al. reference is unrelated to session management within a web farm having multiple servers. Accordingly, the Applicant respectfully requests withdrawal of the Examiner's rejections based upon Williams et al. and Bachman et al. Reconsideration and issuance of a timely Notice of Allowance is earnestly solicited.

Should the Examiner have any questions with regard to the submissions, please contact the Applicant's agent, Fraser Rowand, at 416-868-1482. Should the Examiner be inclined to maintain any of the rejections in a second Office Action, the Applicant respectfully requests the courtesy of a telephone interview to discuss the

grounds for maintaining any rejections over the arguments supplied herein.

Respectfully Submitted,

PETROVIC, Sladjana

By: _____

Fraser D. Rowand, Regn. No.53,870

Place: Toronto, Ontario, Canada
Date: March 20, 2007
Tele No.: 416-868-1482